How to install or update Fortify rulepacks

This page has been made public for vendors

Question

How can I install or update Fortify rulepacks?

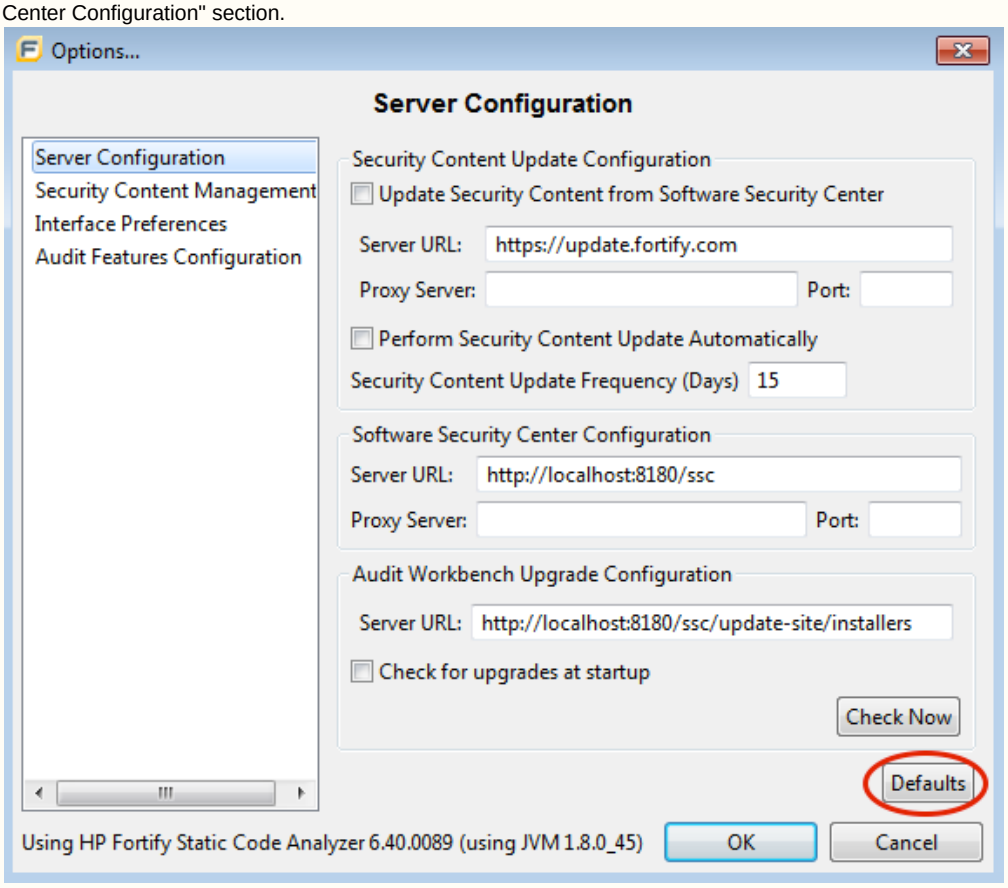
Answer

There are several ways to install or update Fortify rulepacks. Each option will be discussed below.

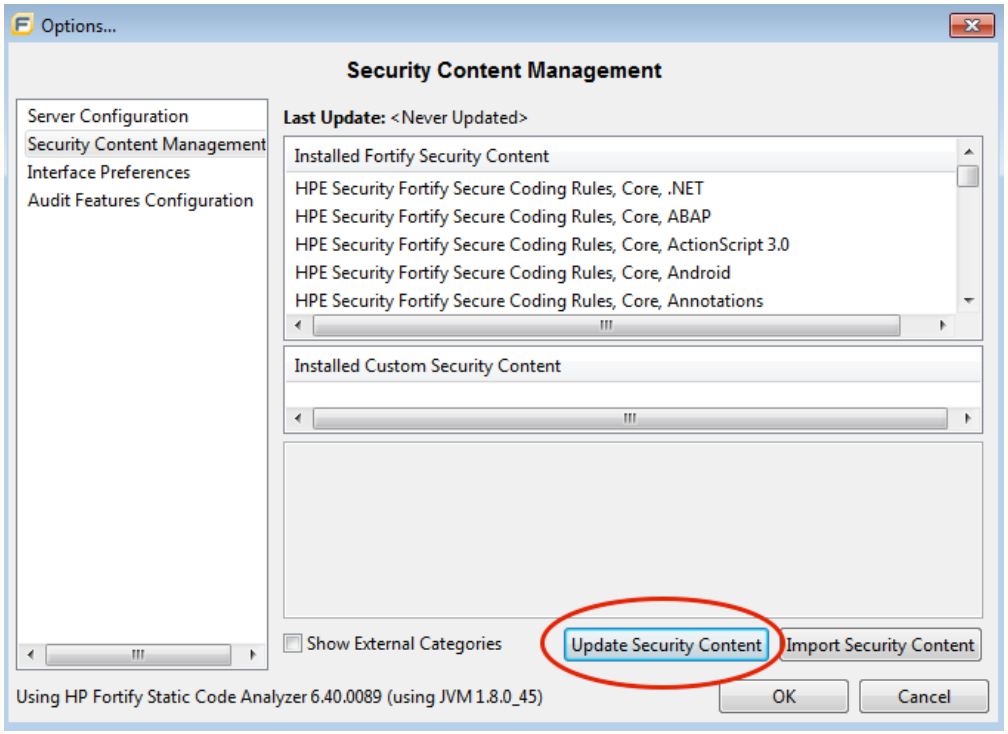
Option 1: Audit Workbench GUI

Fortify rulepacks can be downloaded and installed via the Audit Workbench via the following steps:

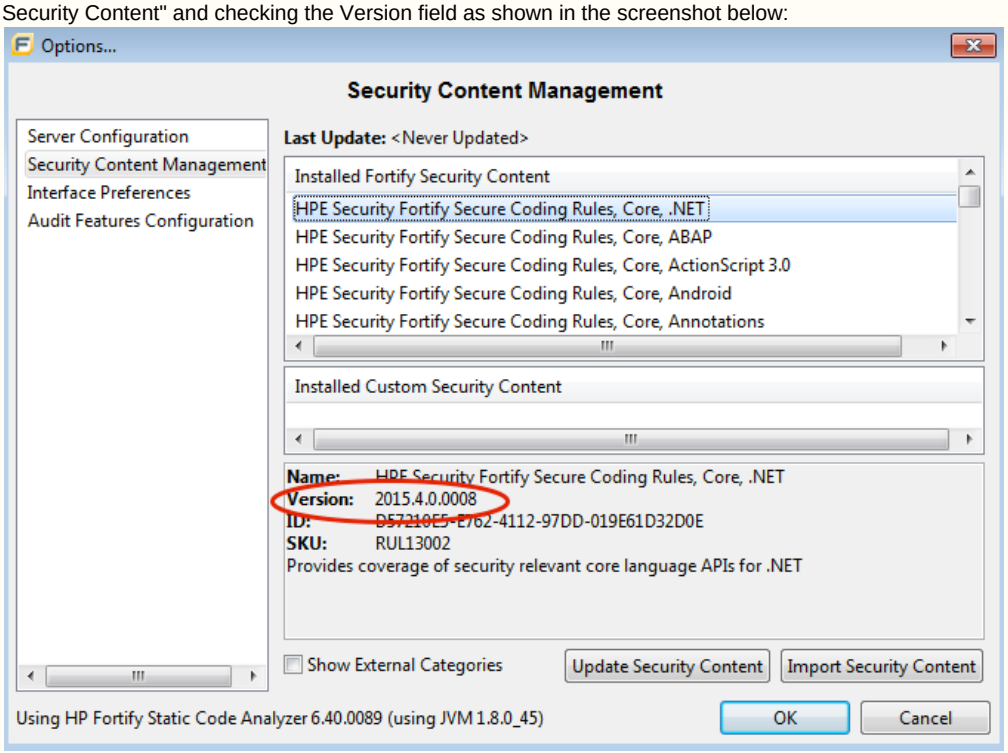
- Open the Audit Workbench.
- From the Options menu, select "Options..."
- Under Server Configuration, ensure the servers are configured correctly. If your team is not using Software Security Center, the default settings are typically correct (update from https://update.fortify.com). You can reset to defaults by clicking the "Defaults" button or changing the configuration to match the screenshot below. If your team is using Software Security Center, check the "Update Security Content from Software Security Center" and specify the correct information under the "Software Security Center Configuration" section.



- After setting the correct Server Configuration, click on "Security Content Management" and click the "Update Security Content" button as shown in the screenshot below:



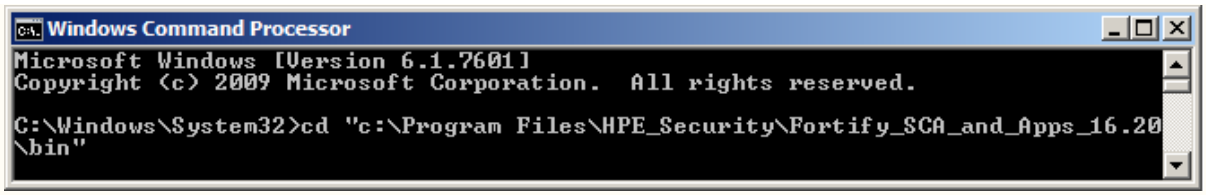
- Once the update process completes, you can check the version installed by selecting one of the items under "Installed Fortify Security Content" and checking the Version field as shown in the screenshot below:



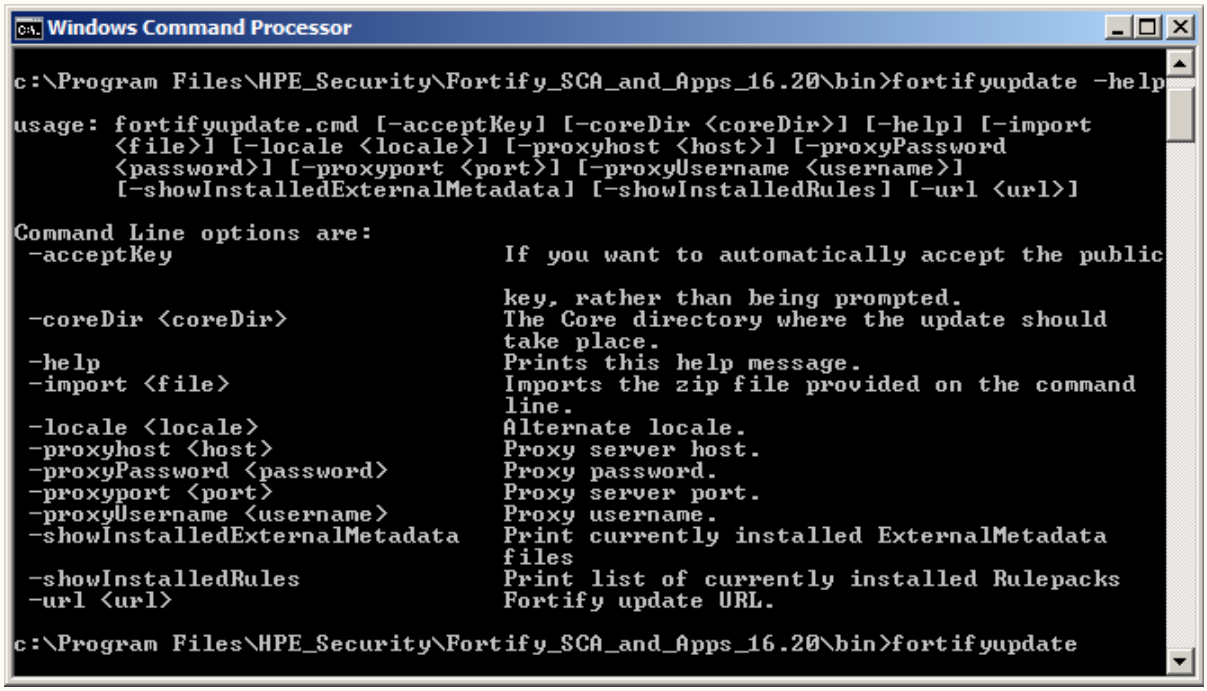
Option 2: Command Line Interface

Alternatively to the Audit Workbench GUI, Fortify rulepacks can also be downloaded and installed via Fortify command line tools as follows:

- Open a command prompt and navigate to the Fortify installation "bin" directory. For example, for Fortify 16.20 on Windows the default "bin" directory path is D:\Program Files\HPE_Security\Fortify_SCA_and_Apps_16.20\bin as in the screenshot below:



- The fortifyupdate command line tool may be used to facilitate the update. This tool provides several options as shown in the screenshot below:



- If your team is not using Software Security Center, the default settings are typically correct (update from https://update.fortify.com). You can explicitly specify this by running the command as: `fortifyupdate -url https://update.fortify.com`
- If your team is using Software Security Center, specify the correct information for your server.
- After running the command, you can verify the installed content and version via the Audit Workbench as shown in Option 1 above.

Option 3: Manual Installation

In some cases, you may be unable to download the rulepacks from Fortify's server. This may occur if your instance of Fortify is installed in an offline environment, or if you encounter firewall blocking issues (e.g. Error 6243). In this scenario, you can request a copy of the latest Fortify rule packs from the VA SwA Office and then manually install the rulepack files. Once you have received the rulepack zip file there two options for installing:

- Option 1: Run the fortifyupdate tool with `fortifyupdate -import <file>` where `<file>` is the name of the zip file.
- Option 2:
  - Extract the contents of the zip file. You should have a collection of .bin files and an ExternalMetadata folder.
  - Copy the .bin files to <Installation_Dir>\Core\config\rules
  - Copy the ExternalMetadata\externalmetadata.xml file to <Installation_Dir>\Core\config\ExternalMetadata

After completing one of the options above, you can verify the installed content and version via the Audit Workbench as shown in Option 1 above.

See Also

- How to open an NSD ticket to request VA-licensed Fortify software
- How to download the VA-Licensed HP Fortify software